PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G10L 9/00, 9/06

A1

(11) International Publication Number: **WO 99/42992**

(43) International Publication Date: 26 August 1999 (26.08.99)

(21) International Application Number: PCT/US99/03976

(22) International Filing Date: 24 February 1999 (24.02.99)

(30) Priority Data:
09/028,243 24 February 1998 (24.02.98) US

(71)(72) Applicant and Inventor: HOLOUBEK, Michael, J. [US/US]; Annapolis Technologies International, 211 Chinquapin Round Road, Annapolis, MD 21401 (US).

(74) Agents: LEINBERG, Gunnar, G. et al.; Nixon Peabody LLP, Clinton Square, P.O. Box 1051, Rochester, NY 14603 (US).

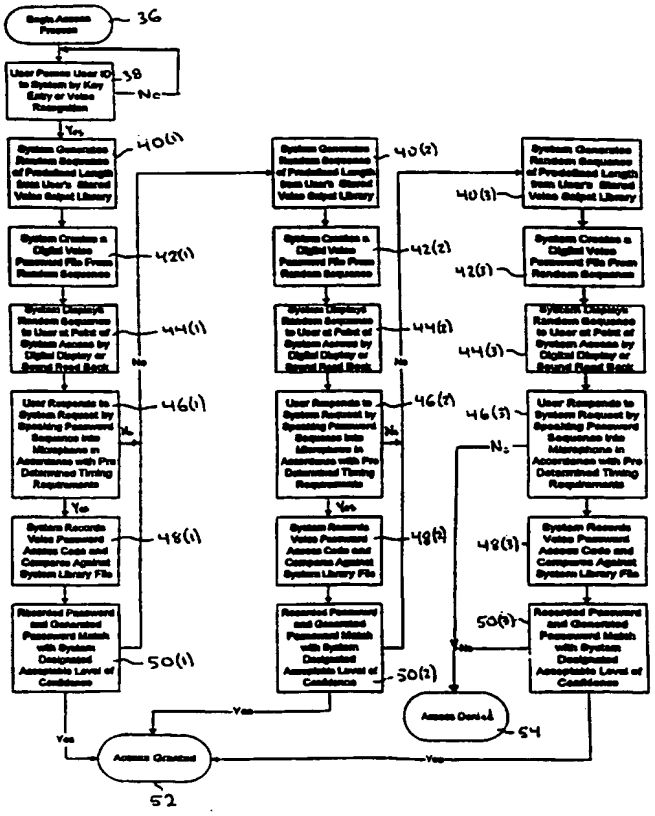
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: RANDOMLY GENERATED VOICE RECOGNITION METHOD AND APPARATUS

(57) Abstract

A voice recognition security method and system in accordance with one embodiment of the present invention has several steps including: storing a set of recorded snippets (40(3)); randomly selecting two or more of the recorded snippets (40(1)); displaying each of the randomly selected recorded snippets (44(1)); requiring each of the randomly selected recorded sinppets to be repeated; comparing each of the repeated snippets against the corresponding randomly selected recorded snippet (48(2)); and determining if access is granted based on these comparisons.



BEST AVAILABLE COPY

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

RANDOMLY GENERATED VOICE RECOGNITION METHOD AND APPARATUS

FIELD OF THE INVENTION

This invention relates generally to security methods and systems and, more particularly, to a randomly generated voice recognition security method and apparatus where one or more passwords are randomly generated from a set of passwords and must be repeated and verified for a user to gain access.

BACKGROUND OF THE INVENTION

Restricted or controlled access to a variety of different systems and areas has become a common part of our daily lives. For example, systems are used to control access to areas, such as our homes and hotel rooms, to financial applications, such as ATM machines and home banking systems and to data, such as corporate, medical, and government records. Historically, access to areas was granted or denied based upon personal recognition. However, as activities, such as banking and shopping, have become less personalized, reliance on other means of identification has become necessary. Currently to gain access, most of systems require ownership of an access card and/or a password or personal identification number (PIN). Although these cards and/or passwords or PINs provide some security, they can easily be compromised.

More sophisticated systems which are more difficult to compromise, such as systems which match biometrics with computers, are now available. These systems use facial, fingerprint and/or voice features in the identification process. Although the first two techniques, facial and fingerprint identification, are effective and can be done remotely without human intervention, they are both complex and expensive requiring the use of sophisticated camera systems as well as high quality transmission media.

The other technique, computer analysis of voice features, can be accomplished with most computers already in use by simply adding the appropriate software. Basically, these systems operate by comparing the utterance

of a password by a person requesting access against a pre-stored utterance of the same password. Access is granted, if the compared utterances are within established tolerances. To further assure proper authentication, some of these systems require a series of passwords to be repeated and authenticated. By way of example, U.S. Patent No. 4,363,102 to Holmgren, U.S. Patent No. 4,581,755 to Sakoe, U.S. Patent No. 4,716,593 to Hirai et al., U.S. Patent No. 5,142,565 to Ruddle, U.S. Patent No. 5,430,827 to Rissanen, and U.S. Patent No. 5,517,558 to Schalk disclose voice recognition systems and methods which are all herein incorporated by reference.

Unfortunately, these voice recognition systems and methods, can easily be defeated. An unauthorized user simply needs to record an authorized user speaking the password and then the unauthorized user simply plays back the tape of the authorized user speaking the password or passwords at the appropriate time during the authentication process to gain access.

One prior system and method to try and overcome this problem requires a requester to repeat a series of utterances containing at least one repeated utterance. The repeated utterances are compared against a prestored template of utterances and the repeated utterances are compared against each other. The requester is authenticated only if each representation of the repeated utterances matches the prestored template to within a predetermined tolerance while the representations of the repeated utterance do not match each other to such a high degree that they are deemed to be mechanically generated. One example of a system and method similar to this is disclosed in U.S. Patent No. 5,265,191 to McNair, which is herein incorporated by reference.

Although this prior system and method is useful in preventing someone from recording an authorized user repeating the passwords and then simply patching the passwords together in the correct order, the system and method can still be defeated. An unauthorized user still simply needs to record the authorized user while he or she is gaining access to the system. At that time the authorized user will repeat the series of passwords, including the repeated utterance. When the tape is replayed, the series of passwords will be within the predetermined

tolerances and since the authorized user repeated the repeated utterance it will not be a match to such a high degree that it will be deemed to be randomly generated.

SUMMARY OF THE INVENTION

A voice recognition method and apparatus in accordance with one embodiment of the present invention has several steps including: storing a set of recorded snippets; randomly selecting two or more of the recorded snippets; displaying each of the randomly selected recorded snippets; requiring each of the randomly selected recorded snippets to be repeated; comparing each of the repeated snippets against the corresponding randomly selected recorded snippet; and determining if access is granted based on these comparisons.

A voice recognition method and apparatus in accordance with another embodiment of the present invention has several steps including: storing an authorized identifier for each authorized party to the system; storing a set of recorded snippets for each of the authorized parties; requiring an inquiring party to enter an inquiring identifier; determining if the inquiring identifier matches one of the authorized identifiers; denying access if the inquiring identifier does not match one of the authorized identifiers; randomly selecting two or more of the recorded snippets for the authorized party whose authorized identifier matched the inquiring identifier; requesting the inquiring party to repeat each of the randomly selected recorded snippets within a first period of time; denying access if any of the randomly selected recorded snippets is not repeated within the first period of time after the request; comparing each of the repeated snippets against the corresponding randomly selected recorded snippet; and determining if access is granted based on each of these comparisons.

The present invention is also directed to a computer program recorded on a computer readable medium for providing security using voice recognition in accordance with another embodiment of the present invention. The program includes a voice recognition source code segment comprising randomly selecting two or more recorded snippets for the authorized identifier which matched the inquiring identifier stored on the computer readable medium. displaying the

randomly selected recorded snippets in series, comparing each repeated snippets against the corresponding randomly selected recorded snippet which was displayed, and determining if access is granted based on each of these comparisons. The computer program recorded on a computer readable medium may also include an identification source code segment comprising determining if an inquiring identifier matches one of a set of one or more authorized identifiers stored on the computer readable medium and denying access if the inquiring identifier does not match one of the authorized identifiers.

The present invention provide a number of advantages including providing a voice recognition method and apparatus which adds a level of security over existing security methods and systems. Unlike existing security methods and systems, with the present invention simply tape recording an individual gaining access and then later replaying the tape will not work. The random selection process for the passwords with the present invention creates a new series or sequence of passwords each time a user tries to gain access. The level of security is further enhanced with the present invention by requiring the authorized parties to periodically change their library of recorded passwords.

Another advantage of the present invention is the incorporation of a time limit during which the user must repeat the displayed password. If the time limit expires before the user repeats a displayed password, then the user is denied access. This prevents unwanted users or intruders from trying to rewind or fast forward to recorded passwords which may have been recorded surreptitiously and are in a different order from that now required by the random generation of passwords by the present invention. With the combination of the randomly generated series of passwords and the time limits, defeating this security method and system with today's technology would be nearly impossible and extremely costly.

Another advantage of the present invention is that it can easily be combined with other security techniques to further enhance the level of security. For example, not only can the method and system generate a random set of passwords to be repeated and verified within a set period of time, but the

randomly generated passwords could be in the form of questions, such as what month was the user born or what is the users dog's name, which would require answers to be repeated which only a few individuals might know adding to the level of security. The present invention could also be combined with prior security techniques and devices, such as the use of an access card which when inserted would then generate a random series of passwords to be repeated and verified within a set period of time.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a simplified block diagram of one embodiment of a randomly generated voice recognition apparatus in accordance with the present invention; and

FIG. 2 is a flow chart illustrating one embodiment of a randomly generated voice recognition method in accordance with the present invention.

DETAILED DESCRIPTION

A randomly generated voice recognition apparatus 10 and method in accordance with one embodiment of the present invention is illustrated in FIGS. 1 and 2. One embodiment of the method includes the steps of storing a set of recorded snippets, randomly selecting two or more of the recorded snippets, displaying each of the randomly selected recorded snippets, requiring each of the randomly selected recorded snippets to be repeated, comparing each of the repeated snippets against the corresponding randomly selected recorded snippet, and then determining if access is granted based on these comparisons. The randomly generated voice recognition apparatus 10 includes a controller or central processing unit (CPU) 12, a memory 14, a random snippet selector 16, a snippet comparator 18, a display 20, and a microphone 22. The randomly generated voice recognition apparatus 10 and method provide a number of advantages including providing a randomly generated series of snippets or passwords each time a user tries to gain access, a time limit in which to repeat each of the randomly generated snippets to further enhance the level of security and a security apparatus 10 and

method which can easily be combined with other security techniques to further enhance the level of security.

Referring to FIG. 1, a simplified block diagram of one embodiment of a randomly generated voice recognition apparatus 10 in accordance with the present invention is illustrated. The apparatus includes CPU or controller 12, memory 14, such as a read only memory and a random access memory, a random snippet selector 16, a snippet comparator 18, a display 20, a microphone 22, an input/output (I/O) device 24, a timer 26, and an optional key pad 28 all coupled together via a bus 30. The CPU or controller 12 operates a computer program which is set forth in greater detail below with reference to FIG. 2 and is stored or embedded in the memory 14 or some other computer readable memory coupled to the CPU 12.

The memory 14 can be a random access memory, a read only memory, or any other type of computer readable memory. In addition to storing the computer program which is set forth in greater detail below with reference to FIG. 2, the memory 14 also stores snippets or passwords, such as "one", "two", "alpha", "bravo", "grass", "sky", "brown", "blue", "what month where you born", "what is your dog's name", etc., for each authorized party or user. Any type of vocal representation, such as a letter, strings of letters, strings of letters and numbers, numbers, partial words, whole words, sentences, in any language can be used and record as a snippet for an authorized party. Each authorized party is recorded speaking each snippet which constitutes that authorized party's library of snippets. The vocal representation of each of the snippets by each of the authorized parties is typically recorded as an analog signal for each snippet which is converted to a digital signal and is then stored in the memory 14. The number of snippets and the type of snippets in each library or structure in memory 14 for each authorized party can vary as needed or desired. To increase the level of security, the number of snippets in memory 14 should be large enough so that it would be difficult, if not impossible, for an intruder or unwanted user to have recorded an authorized party speaking each snippet in a library. For example, in this particular embodiment, each authorized party has between one-hundred to two-hundred

snippets stored in memory. Periodically, each authorized party may be required to replace his/her library of snippets with a new set of snippets. This adds yet another level of security with the present invention. In this particular embodiment, the library of snippets for each authorized party is replaced every thirty to forty-five days, although the replacement period can vary as needed or desired.

The random snippet selector 16 randomly selects two or more snippets stored in memory 14 from the library of the authorized party identified by an inquiring party trying to gain access. The number of randomly selected snippets can vary as needed or desired. The signals representing the randomly selected snippets are transmitted to the display 20 via the bus 30. The random snippet selector 16 transmits the next randomly selected snippet to the display 20 to be displayed, when the previously displayed randomly selected snippet has been repeated and recorded via the microphone 22. The random snippet selector 16 may be implemented using hardware, software, or some combination of both as is readily apparent to one of ordinary skill in the art.

The display 20 receives the signals from the random snippet selector 16 which represent the randomly selected snippets and displays them. Any type of display 20 can be used. For example, the display 20 could be a visual display, such as a cathode ray tube (CRT), a digital screen, or a printer, could be an audio and visual display, such as a CRT with a speaker, or could be an audio display with just a speaker.

The timer 26 is triggered to start running each time one of the randomly selected snippets is displayed by the display 20. If a repeated snippet is not received by the apparatus 10 before a first period of time kept by timer 26 has expired, then access to the inquiring party is denied. In this particular embodiment, the first period of time is about one to two seconds.

The microphone 22 converts the voice of the inquiring party repeating the randomly selected snippets being displayed to an analog signal which represents the repeated snippet and then transmits the analog signal representing the repeated

snippet to an analog-to-digital (A/D) converter 32. The A/D converter 32 converts the analog signal to a digital signal which represents the repeated snippet and is transmitted to the snippet comparator 18

The snippet comparator 18 receives the signal representing the repeated snippet from the microphone 22 via the A/D converter 32 and also receives the corresponding randomly selected snippet from memory 14 which was displayed at the time the repeated snippet was recorded and compares the repeated snippet against the corresponding randomly selected snippet. The snippet comparator 18 will output a difference signal based on this comparison to the CPU 12. If the difference signal is not within accepted tolerances or acceptable levels of confidence, then access will be denied to the inquiring party. The comparison to determine if an inquiring party is denied access can be based upon one comparison between a repeated snippet and the corresponding randomly selected snippet or based upon an evaluation of all of the comparisons of the repeated snippets against their corresponding randomly selected snippet. Techniques for comparing the two voice signals and for establishing tolerances are well known to those of ordinary skill in the art and thus will not be repeated here. The snippet comparator 18 may be implemented using hardware, software, or some combination of both as is readily apparent to one of ordinary skill in the art.

An optional keypad 28 may also be coupled to the bus 30 and used to permit an inquiring party to punch in an inquiring identifier, such as initials or the user's last name, to identify himself or herself as one of the authorized parties. The inquiring identifier is compared against the set of authorized identifiers stored in memory 14. If the inquiring identifier does not match one of the authorized identifiers, then access is denied and the inquiring party is not permitted to begin the voice recognition process. Alternatively, the microphone 22 may be used to permit an inquiring party to identify himself or herself as one of the authorized parties. In this case, the voice signal representing the inquiring party is compared against voice signals stored for authorized parties in memory 14. Again, if a match is not found, then access is denied.

The apparatus 10 is used to protect a system or area 34, such as a bank ATM, a corporate database, or a home where the apparatus controls the operation of the lock to get into the home. The apparatus 10 is coupled to the protected system or area 34 via an I/O device 24.

Referring to FIG. 2, the method begins with step 36 where the system is activated. In step 38, the user attempting to gain access is required to identify himself or herself. This identification process can be accomplished in a number of different ways well known to those of ordinary skill in the art. For example, the inquiring party or user may enter via the keypad 28 the inquiring party's initials, last name or some other identifying password which is then compared against a list of authorized parties stored in memory 14. Alternatively, the inquiring party might speak his or her name, initials, or some other passwords into the microphone 22 which is then compared against a voice recordings of authorized parties stored in memory 14. Further, the inquiring party might simply swipe a card through a magnetic reader (not shown) and the signal obtained by swiping the card through the magnetic reader is compared against ones stored in memory 14 for authorized parties. If the identifying information entered by the inquiring party does not match with any of the identifying information for the authorized parties stored in memory 14, then the inquiring party is denied access and the No branch is taken. If the information entered identifying the inquiring party matches identifying information for one of the authorized parties stored in memory 14, then the Yes branch is taken.

Next in step 40(1), the random snippet selector 16 randomly selects or generates a series of two or more randomly selected recorded snippets from the set of recorded snippets which are assigned to the authorized party identified by the inquiring party in step 38. The recorded snippets for each of the authorized parties which have permission to access the system are stored in memory 14. Once the recorded snippets have been randomly selected, in step 42(1) a digital voice password file is formed from the randomly selected recorded snippets. In this particular embodiment, the digital voice password file comprises of three snippets, although the number of snippets can vary as needed or desired.

Preferably, in steps 42(2) and 42(3) the digital voice password file will have progressively larger numbers of snippets. For example, the digital voice password file may have four snippets in step 42(2) and may have five snippets in step 42(3). The rationale for this is that there is a stronger probability that an intruder (i.e. unauthorized user) is trying to gain access if a failure is encountered on the first pass, so subsequent passes should be more difficult.

Next in step 44(1), the signals representing the randomly selected recorded snippets are transmitted to the display 20. The display 20 presents the randomly selected recorded snippets to the inquiring party. As discussed earlier, the randomly selected recorded snippets can be displayed in a number of different ways. For example, the randomly selected recorded snippets could be shown on a digital display screen, could be read out via a speaker, or some other visual and audio combination. The randomly selected recorded snippets are displayed one at a time.

Next in step 46(1), the inquiring party responds to the display of the randomly selected recorded snippets by repeating each one as it appears into a microphone within a predetermined period of time. The inquiring party's vocal representations of each randomly selected recorded snippet is recorded, typically as an analog signal which is then converted to a digital signal. A timer 26 is trigger to start running each time a randomly selected recorded snippet is displayed. If the inquiring party does not respond to the display of one of the randomly selected recorded snippets by repeating it within a first period of time, then the No branch is taken and the inquiring party is denied access. By way of example, in this particular embodiment the first period of time is about one and two seconds. If the inquiring party does respond to the display of each of the randomly selected recorded snippets by repeating each of them into microphone 22 within a first period of time, then the Yes branch is taken. The time limit for responding provides an added level of security because it prevents intruders or unauthorized parties from trying to rewind or fast forward to snippets which were surreptitiously recorded from an authorized party, but which because of the

random selection of snippets are not in the correct sequence required for gaining access this time.

Next in steps 48(1) and 50(1), the repeated snippets, which are signals which represent recordings of the inquiring party repeating the randomly selected snippets, are transmitted to the snippet comparator 18. The snippet comparator 18 also receives signals which represent the corresponding randomly selected recorded snippet which was on display at the time the repeated snippet was recorded. The snippet comparator 18 compares the signal which represents the repeated snippet against the signal which represents the corresponding randomly selected recorded snippet which was on display at the time the repeated snippet and produces a difference signal for each comparison in a manner well known to those of ordinary skill in the art. Based on these comparisons, if the difference signals are within established limits or an acceptable level of confidence, then the Yes branch is taken and access is granted in step 52. If the difference signals are not within established limits or an acceptable level of confidence, then the No branch is taken. Again, techniques for analyzing the difference signals and establishing an acceptable level of confidence are well know to those of ordinary skill in the art. A variety of different types of analyses could be used to grant or deny access. For example, the system could deny access based on one of the comparisons of the repeated snippet and the corresponding randomly selected recorded snippet or based on an analysis of all of the comparisons of the repeated snippets against their corresponding randomly selected recorded snippet.

If access is denied and the No branch is taken, the inquiring party may be permitted a limited number of retrys to pass the voice recognition process. Steps 40(2), 42(2), 44(2), 46(2), 48(2), and 50(2) are repeated and if the acceptable level of confidence based on the comparison of the new set of repeated snippets and randomly selected recorded snippets is reached, then the Yes branch is taken and access is granted in step 52. If the acceptable level of confidence is still not reached, then the No branch is taken and the inquiring party may be provided one more opportunity to gain access. If following steps 40(3), 42(3), 44(3), 46(3), 48(3), and 50(3), the acceptable level of confidence based on the comparison of

the another new set of repeated snippets and randomly selected recorded snippets is reached, then the Yes branch is taken and access is granted in step 52. If the acceptable level of confidence is still not reached, then the No branch is taken and the inquiring party is denied access in step 54. Steps 40(2), 42(2), 44(2), 46(2), 48(2), and 50(2) and steps 40(3), 42(3), 44(3), 46(3), 48(3), and 50(3) are identical to steps 40(1), 42(1), 44(1), 46(1), 48(1), and 50(1) and thus will not be described again here. Although in this particular embodiment, the inquiring party is permitted two additional attempts to satisfy the voice recognition requirements to gain access, the number of retrys can be made higher or lower as needed or desired.

Having thus described the basic concept of the invention, it will be rather apparent to those skilled in the art that the foregoing detailed disclosure is intended to be presented by way of example only, and is not limiting. Various alternations, improvements, and modifications will occur and are intended to those skilled in the art, though not expressly stated herein. These alterations, improvements, and modifications are intended to be suggested hereby, and are within the spirit and scope of the invention. Accordingly, the invention is limited only by the following claims and equivalents thereto.

CLAIMS

What Is Claimed Is:

1. A method for providing a voice recognition security system, the method comprising:

storing a set of recorded snippets;

randomly selecting two or more of the recorded snippets;

displaying each of the randomly selected recorded snippets;

requiring each of the randomly selected recorded snippets to be repeated;

comparing each of the repeated snippets against the corresponding randomly selected recorded snippet; and

determining if access is granted based on these comparisons.

2. The method according to claim 1 further comprising:

storing a set of one or more authorized parties, wherein each of the authorized parties has its own set of the recorded snippets;

determining if an inquiring party attempting to gain access is in the set of authorized parties; and

denying access if the inquiring party is not one of the authorized parties.

3. The method according to claim 2 further comprising requiring each of the authorized parties to record a new set of randomly selected recorded snippets after a first period of time.

4. The method according to claim 1 wherein the step of requiring each of the randomly generated selected snippets to be repeated further comprises the steps of:

requiring each of the randomly generated recorded snippets to be repeated within a second period of time after each of the randomly selected snippets is displayed; and

denying access if any of the randomly selected recorded snippets is not repeated within the second period of time.

5. The method according to claim 5 wherein the second period of time is about one to two seconds.

6. The method according to claim 5 wherein the steps of storing a set of recorded snippets, randomly selecting two or more of the recorded snippets,

displaying each of the randomly selected recorded snippets, requiring each of the randomly selected recorded snippets to be repeated, comparing each of the repeated snippets against the corresponding recorded snippet, and determining if access is granted based on these comparisons are repeated a set number of times when access is denied because one of the randomly selected recorded snippets is not repeated within the second period of time.

7. The method according to claim 6 wherein the set number of times is two.

8. The method according to claim 1 wherein the steps of storing a set of recorded snippets, randomly selecting two or more of the recorded snippets,

displaying each of the randomly selected recorded snippets, requiring each of the randomly selected recorded snippets to be repeated, comparing each of the repeated snippets against the corresponding recorded snippet, and determining if access is granted based on these comparisons are repeated a set number of times when access is denied because of the comparison of the repeated snippets against the recorded snippets.

9. The method according to claim 8 wherein the set number of times is two.

10. A method for providing security to a system using voice recognition, the method comprising:

storing an authorized identifier for each authorized party to the system;

storing a set of recorded snippets for each of the authorized parties;

requiring an inquiring party to enter an inquiring identifier;

determining if the inquiring identifier matches one of the authorized identifiers;

denying access if the inquiring identifier does not match one of the authorized identifiers;

randomly selecting two or more of the recorded snippets for the authorized party whose authorized identifier matched the inquiring identifier;

requesting the inquiring party to repeat each of the randomly selected recorded snippets within a first period of time;

denying access if any of the randomly selected recorded snippets is not repeated within the first period of time after the request;

comparing each of the repeated snippets against the corresponding randomly selected recorded snippet; and

determining if access is granted based on each of these comparisons.

11. The method according to claim 10 wherein the first period of time is about one to two seconds.

12. The method according to claim 10 further comprising requiring each of the authorized parties to record a new set of randomly selected recorded snippets after a second period of time.

13. The method according to claim 10 wherein the steps of randomly selecting two or more of the recorded snippets for the authorized party whose authorized identifier matched the inquiring identifier, displaying the randomly selected recorded snippets in series, requiring the inquiring party to repeat each of the randomly selected recorded snippets within a first period of time, denying access if any of the randomly selected recorded snippets is not repeated within the first period of time, and comparing each of the repeated snippets against the corresponding recorded snippet are repeated a set number of times when access is denied because one of the randomly selected recorded snippets is not repeated within the first period of time.

14. The method according to claim 10 wherein the steps of randomly selecting two or more of the recorded snippets for the authorized party whose authorized identifier matched the inquiring identifier, displaying the randomly selected recorded snippets in series, requiring the inquiring party to repeat each of the randomly selected recorded snippets within a first period of time, denying access if any of the randomly selected recorded snippets is not repeated within the first period of time, and comparing each of the repeated snippets against the corresponding recorded snippet are repeated a set number of times when access is denied because of the comparison of the repeated snippets against the randomly selected recorded snippets.

15. An apparatus for providing a voice recognition security system, the apparatus comprising:

means for storing a set of recorded snippets;

means for randomly selecting two or more of the recorded snippets;

means for displaying each of the randomly selected recorded snippets;

means for requiring each of the randomly selected recorded snippets to be repeated;

means for comparing each of the repeated snippets against the corresponding recorded snippet; and

means for determining if access is granted based on these comparisons.

16. The apparatus according to claim 15 further comprising:

means for storing a set of one or more authorized parties, wherein each of the authorized parties has its own set of the recorded snippets;

means for determining if an inquiring party attempting to gain access is in the set of authorized parties; and

means for denying access if the inquiring party is not one of the authorized parties.

17. The apparatus according to claim 16 further comprising means for requiring each of the authorized parties to record a new set of randomly selected recorded snippets after a first period of time.

18. The apparatus according to claim 15 wherein the means for requiring each of the randomly generated selected snippets to be repeated further comprises:

means for requiring each of the randomly generated recorded snippets to be repeated within a second period of time after each of the randomly selected snippets is displayed; and

means for denying access if any of the randomly selected recorded snippets is not repeated within the second period of time.

19. The apparatus according to claim 18 wherein the second period of time is about one to two seconds.

20. An apparatus for providing security using voice recognition comprising:

means for storing an authorized identifier for each authorized party;

means for storing a set of recorded snippets for each of the authorized parties;

means for requiring an inquiring party to enter an inquiring identifier;

means for determining if the inquiring identifier matches one of the authorized identifiers;

means for denying access if the inquiring identifier does not match one of the authorized identifiers;

means for randomly selecting two or more of the recorded snippets for the authorized party whose authorized identifier matched the inquiring identifier;

means for displaying the randomly selected recorded snippets in series;

means for requiring the inquiring party to repeat each of the randomly selected recorded snippets within a first period of time;

means for denying access if any of the randomly selected recorded snippets is not repeated within the first period of time.

means for comparing each of the repeated snippets against the corresponding recorded snippet; and

means for determining if access is granted based on each of these comparisons.

21. The apparatus according to claim 20 wherein the first period of time is about one to two seconds.

22. The apparatus according to claim 20 further comprising means for requiring each of the authorized parties to record a new set of randomly selected recorded snippets after a second period of time.

23. A computer program recorded on a computer readable medium for providing security using voice recognition comprising a voice recognition source code segment comprising randomly selecting two or more recorded snippets for the authorized identifier which matched the inquiring identifier stored on the computer readable medium, displaying the randomly selected recorded snippets in series, comparing each repeated snippets against the corresponding recorded snippet which was displayed, and determining if access is granted based on each of these comparisons.

24. The computer program as set forth in claim 23 wherein the voice recognition source code segment further comprises denying access if any of the randomly selected recorded snippets being displayed is not repeated within a first period of time.

25. The computer programs according to claim 24 wherein the first period of time is about one to two seconds.

26. The computer programs according to claim 23 further comprising an identification source code segment comprising determining if an inquiring

identifier matches one of a set of one or more authorized identifiers stored on the computer readable medium and denying access if the inquiring identifier does not match one of the authorized identifiers

27. A computer program recorded on a computer readable medium for providing security using voice recognition comprising:

an identification source code segment comprising requesting an inquiring identifier, determining if the inquiring identifier matches one of a set of one or more authorized identifiers, and denying access if the inquiring identifier does not match one of the authorized identifiers; and

a voice recognition source code segment comprising randomly selecting two or more recorded snippets for the authorized identifier which matched the inquiring identifier, requesting a repeated snippet for each of the randomly selected recorded snippets, comparing each of the repeated snippets against the corresponding randomly selected recorded snippet, and determining if access is granted based on each of these comparisons.

28. The computer program as set forth in claim 27 wherein the voice recognition source code segment further comprises denying access if any of the randomly selected recorded snippets being displayed is not repeated within a first period of time after the request.

29. The computer programs according to claim 28 wherein the first period of time is about one to two seconds.

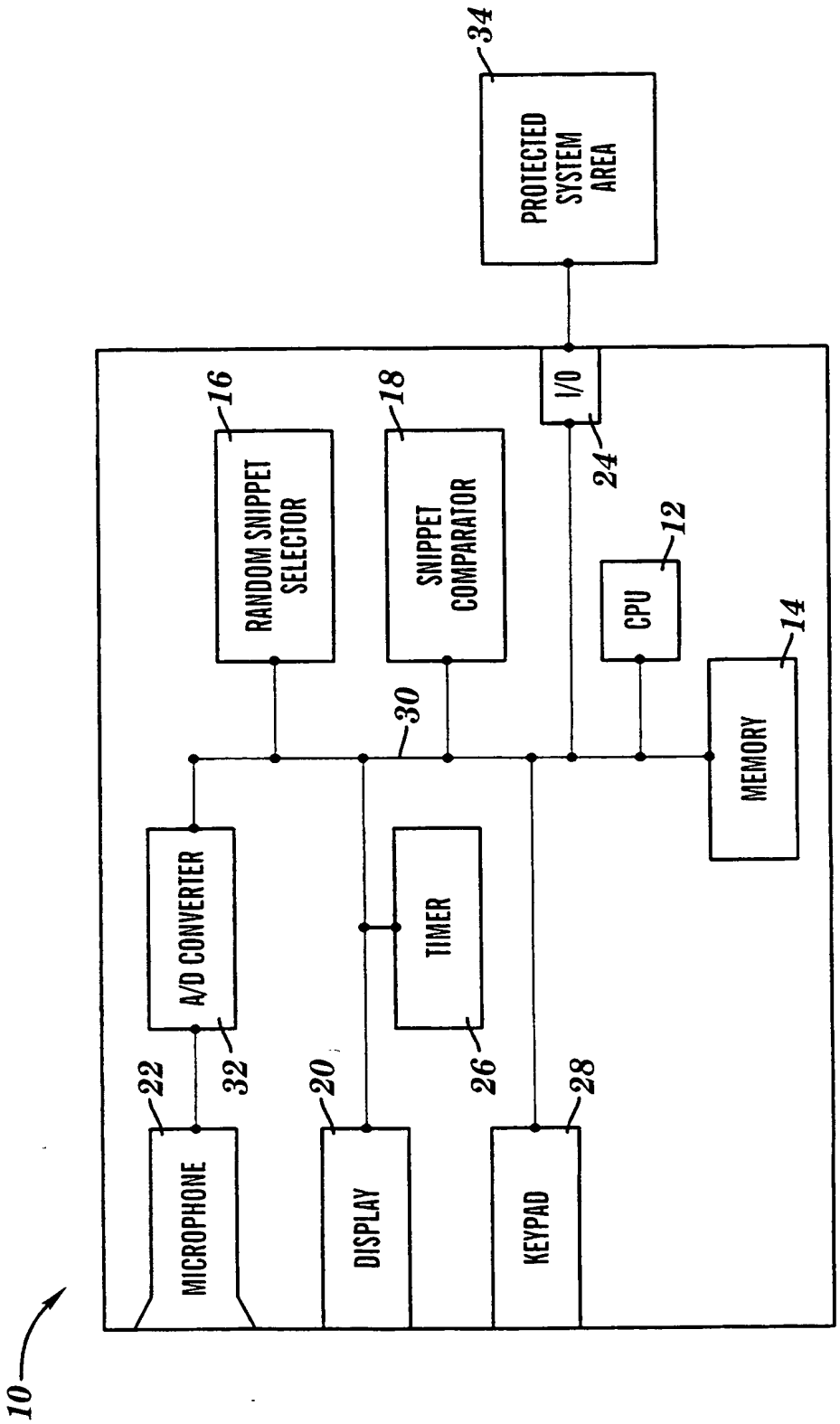


FIG. 1

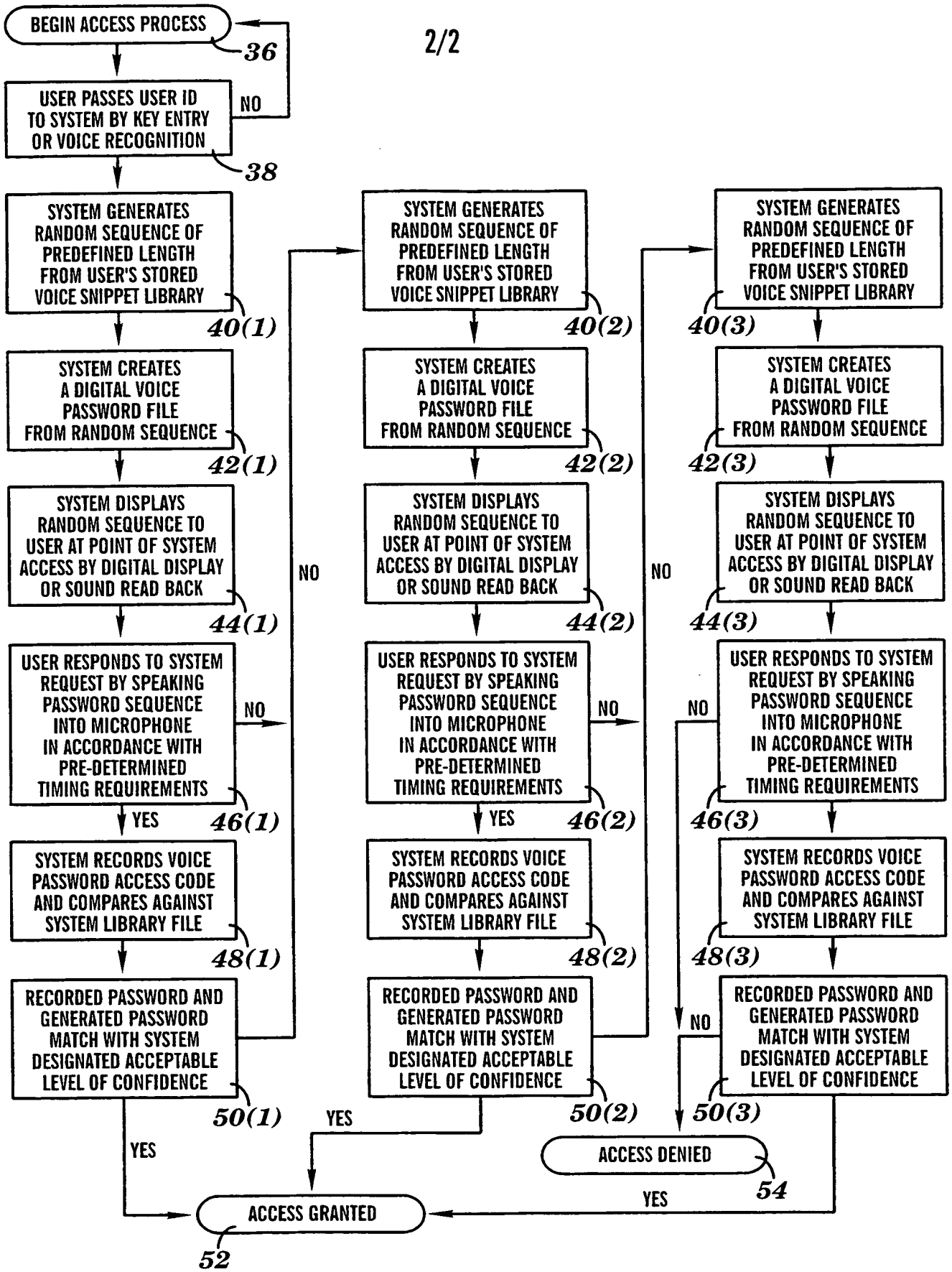


FIG. 2

SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

I national application No.
PCT/US99/03976

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G10L 9/00,9/06
US CL : 704/246,270,273,275

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 704/246,270,273,275

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, IEEE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,430,827 A (HIGGINS) 16 August 1994, col. 2 lines 12-40	1,8,15,23
Y	US 5,430,827 A (HIGGINS) 16 August 1994, col. 2 lines 12-40	2, 4, 6-7, 9-10, 13-14, 16, 18, 20, 24, 26-28
Y	US 5,430,827 A (RISSANEN) 04 July 1995, col. 2 lines 10-41, col. 6 line 56 - col. 7 line 30	2,4,6-7, 9-10, 13-14, 16, 18, 20, 24, 26-28
Y	US 5,465,290 A (HAMPTON et al) 07 November 1995, col. 6 lines 25-42	3,5,11,12,17,19,21,22,25,29
Y	US 5,606,663 A (KADOOKA) 25 Feb 1997, col. 1 lines 19-37	3,5,11,12,17,19,21,22,25,29

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report 23 APR 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No.	Authorized officer DAVID HUDSPETH Telephone No.

Form PCT/ISA/210 (second sheet)(July 1992) *